

- Spam mesajlara kısaca istenmeyen mesajlar denir. Bir eposta kullanıcısının rızası olmadan , değişik amaçlara sahip (siyasi, reklam vb.) epostaların , eposta kullanıcısına gelmesi ve giderek bu eposta trafiğinin artmasına da Spam denebilir.
- Spam Mesajları göndermenin etkin 2 ve dolaylı 1 yöntemi vardır.
 - Spam atan kişilerin kendi SMTP sunucularını, PPP,ADSL ve benzeri bağlantı şekilleri ile kullanıp, gerçek olmayan Host İsmi ve IP ile göndermeleri.
 - Spam atan kişilerin internet üzerinde RELAY'a açık (Bu SMTP sunucusunu herkes kullanır ve bu eposta sunucusu üzerinden eposta atar.) SMTP sunucularını bulup, sistem yöneticilerinin haberi olmadan eposta atmalarıdır.
 - Dolaylı yöntem ise, kişilerin virus yazmaları ve bu viruslerin sistemlere bulaşıp, kişilerin istekleri dışında sistemlerini tarayarak , ilgili ilgisiz herkese eposta atmalarıdır.

Spam ATMA Senaryosu !

Normal Mesaj Alıcısı

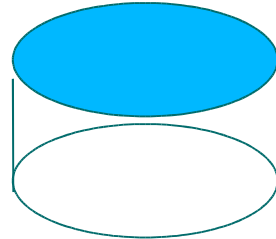


1.) Normal Eposta atma aşaması. İzin verilmiş.



Normal Mesaj
Göndericisi

IP=10.0.0.1



RELAY'a Açık
Eposta Sunucusu

Spam Alıcısı



2.) Spam Eposta atma aşaması. İzin verilmemiş.



Eposta içeriği:
10.0.0.1

Spam Göndericisi



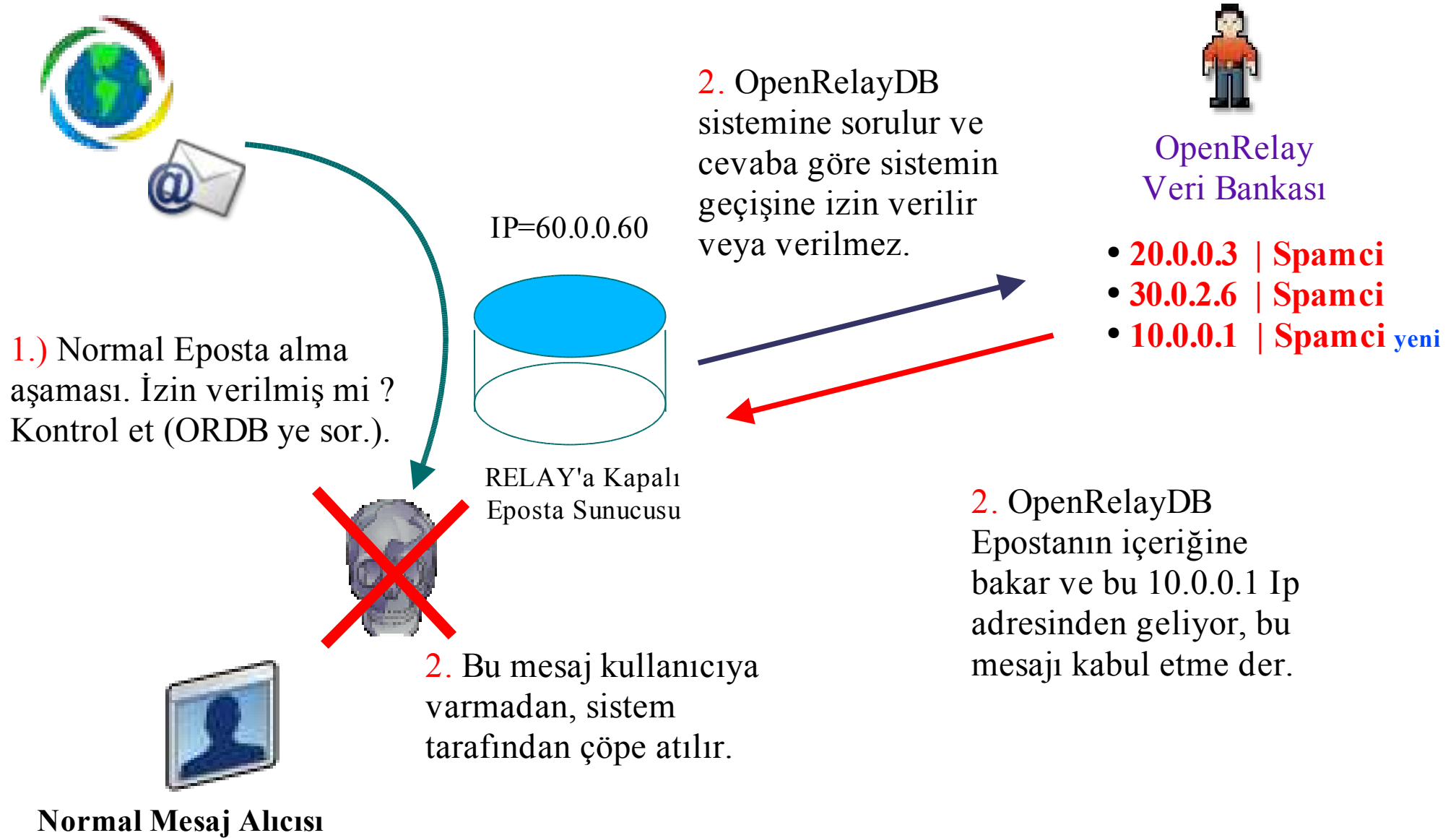
2.a) Spam Eposta almış olan bu kullanıcı maili OpenRelayDB sitesine gönderir.



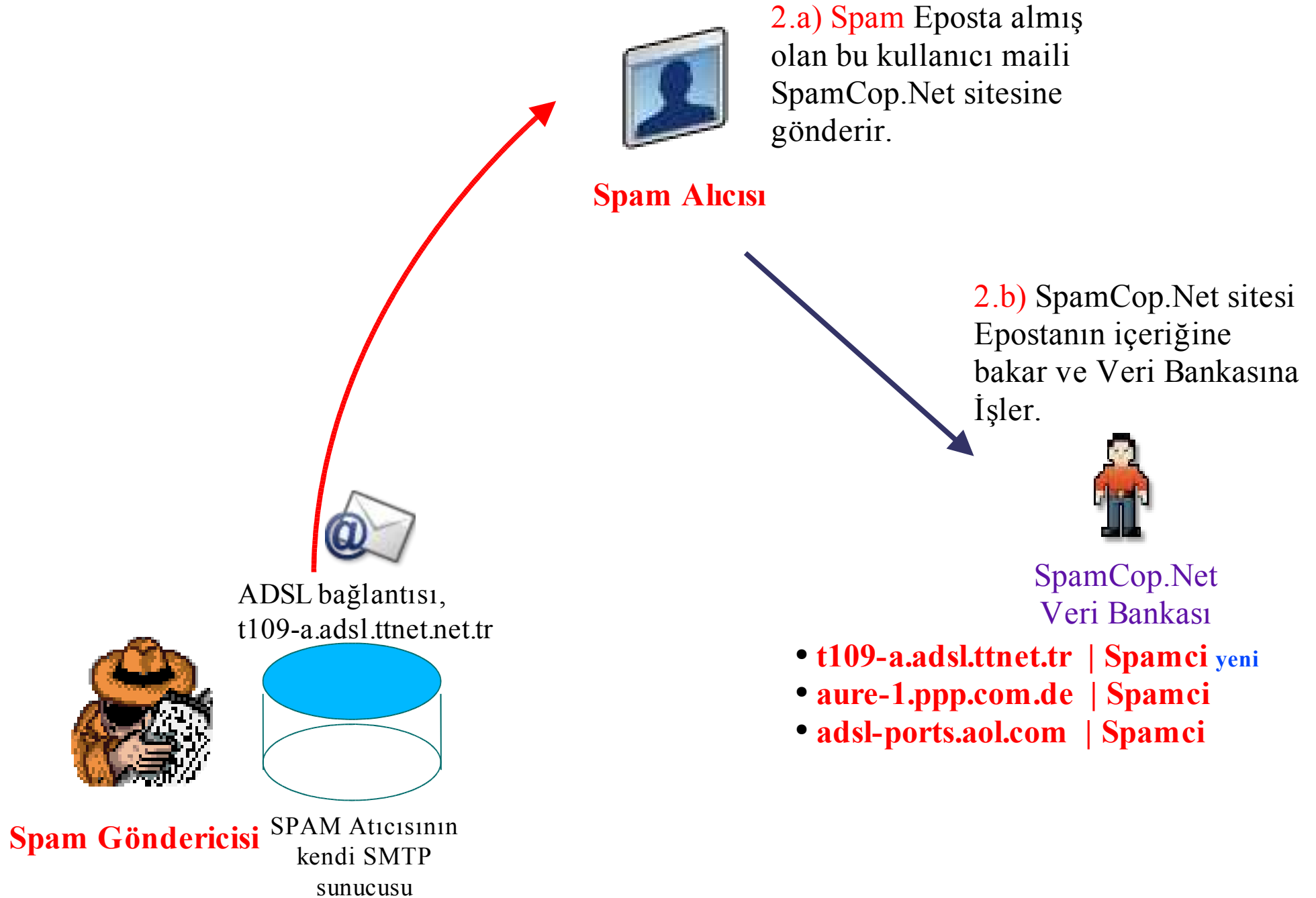
OpenRelay
Veri Bankası

- 20.0.0.3 | Spamci
- 30.0.2.6 | Spamci
- 10.0.0.1 | Spamci yeni

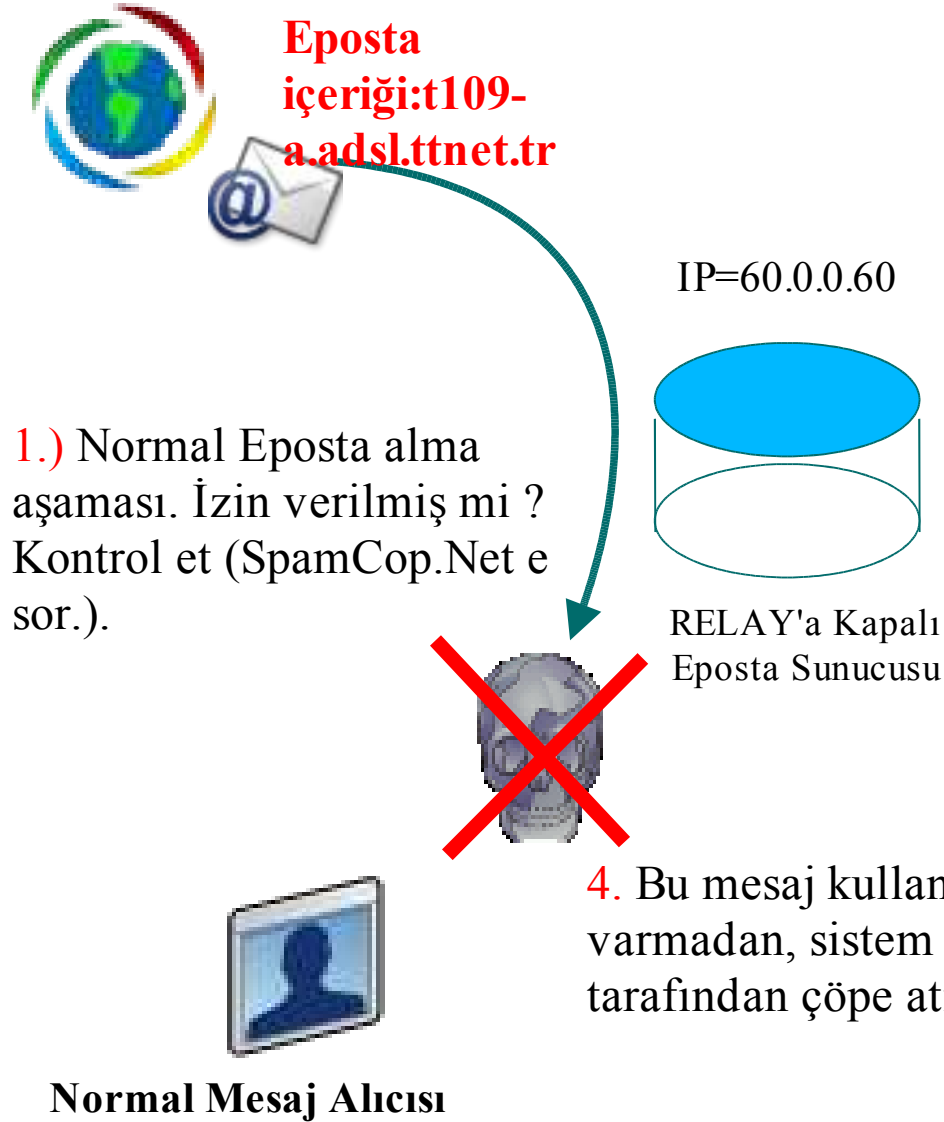
Spam ALMA Senaryosu ORDB Kullanımı



Spam ATMA Senaryosu 2 !



Spam ALMA Senaryosu RBL Kullanımı



2. SpamCop.Net sistemine sorulur ve cevaba göre sistemin geçişine izin verilir veya verilmez.



SpamCop.Net
Veri Bankası

- **t109-a.adsl.ttnet.tr** | Spamci yeni
- **aure-1.ppp.com.de** | Spamci
- **adsl-ports.aol.com** | Spamci

3. SpamCop.Net Epostanın içeriğine bakar ve bu **t109-a.adsl.ttnet.tr** adresinden geliyor, bu mesajı kabul etmez.

Relay Spam Mesajının İçeriği

From – Mon May 26 11:28:40 2003

X-UIDL: <]B"!VR["!h"e!!B1\!!

X-Mozilla-Status: 0003

X-Mozilla-Status2: 00000000

Return-Path: <**spamci@yahoo.com**>

Received: (from root@localhost)

by yahoo (8.12.6p2/8.12.8) id h4Q8FgAw056640;

Mon, 26 May 2003 11:15:42 +0300 (EEST)

(envelope-from **spamci@yahoo.com**)

Received: from **yahoo.com** ([**10.0.0.1**])

by mx.ihotmail.com (qmail-1.03) with SMTP id h4Q8FfCr056630;

Mon, 26 May 2003 11:15:41 +0300 (EEST)

(envelope-from spamci@yahoo.com)

Message-ID: <002a01c3235f\$f6500350\$6658afd4@yahoo.com>

From: "Mujdat Gezen" <**spamci@yahoo.com**>

To: <ustuntas@ihotmail.com>

Subject: Bu bir spam maildir..

Date: Mon, 26 May 2003 11:22:35 +0300

MIME-Version: 1.0

Content-Type: multipart/alternative;

boundary="-----=_NextPart_000_0027_01C32379.1B758F10"

Falan Filan

•10.0.0.1 Adresi Yahoo.com'a ait değil.

RELAY özelliği kullanılarak atılmış.

•10.0.0.1 IP -> Domain İsim sorgusu yapılırsa, IP sahibinin domani farklı çıkar.

Relay Spam Mesajının İçeriği

From – Mon May 26 11:28:40 2003

X-UIDL: <]B"!VR["!h"e!!B1\!!

X-Mozilla-Status: 0003

X-Mozilla-Status2: 00000000

Return-Path: <**xxxxx@spamci.com**>

Received: (from root@localhost)

by yahoo (8.12.6p2/8.12.8) id h4Q8FgAw056640;

Mon, 26 May 2003 11:15:42 +0300 (EEST)

(envelope-from xxxxx@**yahoo.com**)

Received: from **yahoo.com** ([**t109-a.adsl.ttnet.tr**])

by mx.ihotmail.com (qmail-1.03) with SMTP id h4Q8FfCr056630;

Mon, 26 May 2003 11:15:41 +0300 (EEST)

(envelope-from spamci@yahoo.com)

Message-ID: <002a01c3235f\$f6500350\$6658afd4@yahoo.com>

From: "Cem YILMAZ" <xxxxx@**yahoo.com**>

To: <ustuntas@ihotmail.com>

Subject: Bu bir spam maildir..

Date: Mon, 26 May 2003 11:22:35 +0300

MIME-Version: 1.0

Content-Type: multipart/alternative;

boundary="-----=_NextPart_000_0027_01C32379.1B758F10"

Falan Filan

•**t109-a.adsl.ttnet.tr** Adresi Yahoo.com'a ait değil. RBL özelliği kullanılarak atılmış.

•**t109-a.adsl.ttnet.tr** Domain -> IP sorgusu yapılırsa, IP sahibinin domanı, bize bu mailin hangi ISP üzerinden atıldığını gösterir.

OpenRELAY DATABASE (ordb.org) : Relay'a açık eposta sunucularını veri bankasında tutan ve ihtiyacı olan insanlara sunan bir organizasyon.

Relay : Bir Eposta Sunucusunun kullanılarak Eposta Atılma işlemi .(Spam atıcıları sistemin güvenlik açıklarını kullanarak veya sistemin herkese eposta atma hakkını kullanarak attıkları mesajlara OpenRELAY Spam denir)

RBL (RealTimeBlackList) : Kendi eposta sunucularını kullanarak, internete bağlandıkları ISP'nin kaynakları vasıtası ile SPAM eposta atılması sonucunda belirli organizasyonların oluşturdukları veri bankası .
(SpamCop.net)

Murat Üstüntaş

murat[at]ustuntas[nokta]net